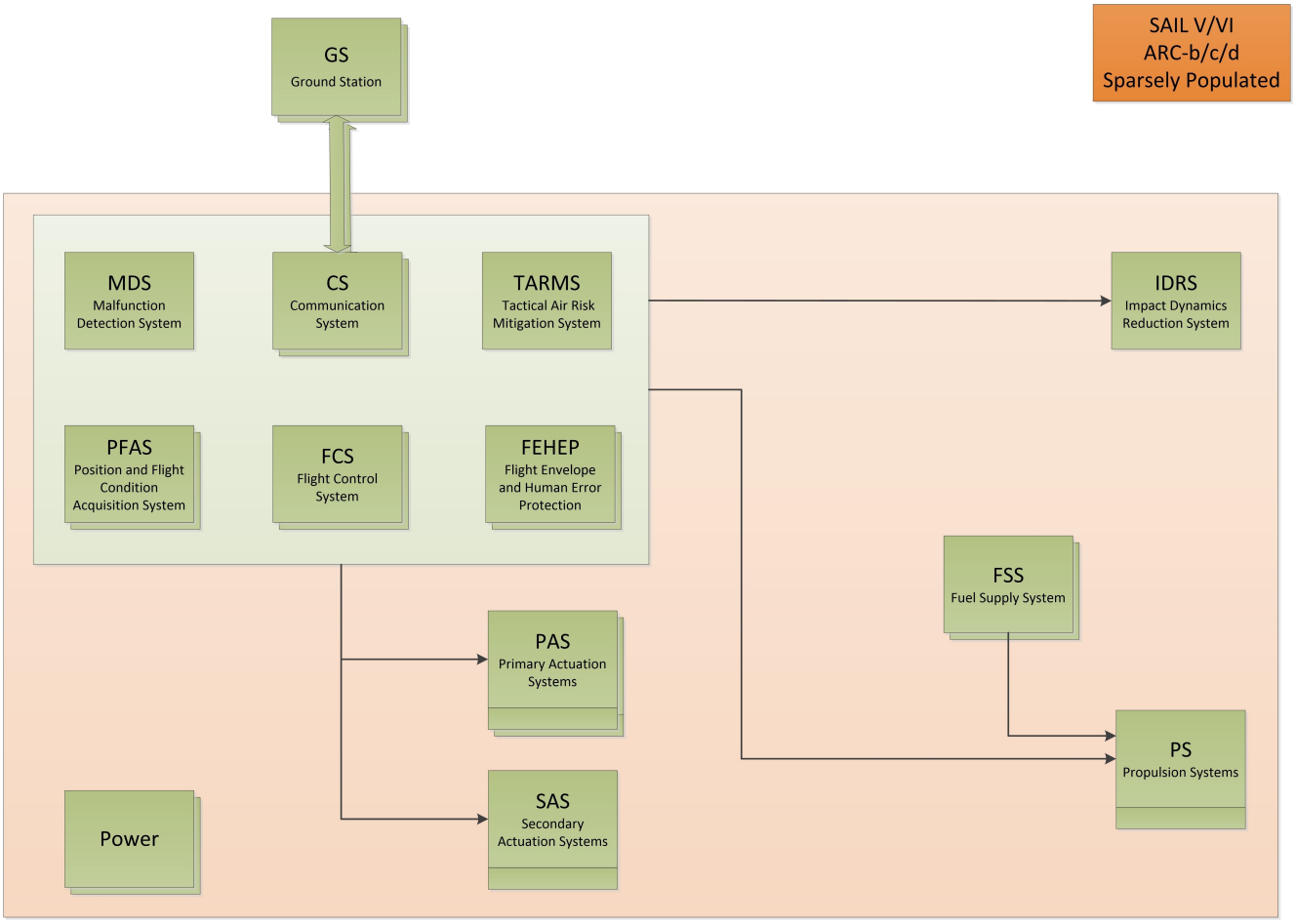
Technische Universität Braunschweig

Deutsches Zentrum für Luft- und Raumfahrt



Development of system architectures on the basis of SORA in the Specific Category and qualitative estimation of the implementation efforts

Institut für Flugsystemtechnik

Daniel Rothe

February 29, 2020

Deutsches Zentrum
DLR für Luft- und Raumfahrt

Entwicklung von Systemarchitekturen auf Basis des SORA in der Specific Category und qualitative Abschätzung der Umsetzungsaufwände

Development of system architectures on the basis of SORA in the Specific Category and qualitative estimation of the implementation efforts

In der Nutzung unbemannter Luftfahrzeuge (UAS) hat sich in den vergangenen Jahren viel getan. Unterschiedlichste Anwendungsszenarien, angefangen bei hobbymäßigen Einsätzen von Kameradrohnen über kommerzielle Anwendungsgebiete wie der Inspektionen von Gebäuden, Windkraftanlagen oder Brücken bis hin zum Langstreckentransport von Gütern haben sich entwickelt. Um diese breit gefächerten Anwendungsszenarien besser zu handhaben hat die EASA 2015 drei neue Kategorien der UAS Regulierung eingeführt: *Open*, *Specific* und *Certified*. Während die Kategorie *Open* im Wesentlichen Spielzeugdrohen und Modellflugzeuge abdeckt und die Kategorie *Certified* Szenarien abdeckt, die ein zur bemannten Luftfahrt vergleichbares Risiko aufweisen, stellt die Kategorie *Specific* einen weit gefächerten Übergang zwischen den beiden anderen Kategorien dar.
Innerhalb der Kategorie *Specific* fordert die EASA ein auf den geplanten Einsatz zugeschnittenes Risiko Assessment zu dem das von der Joint Authorities for Rulemaking of Unmanned Systems (JARUS) entwickelte Specific Operations Risk Assessment (SORA) ein von der Behörde anerkanntes Verfahren darstellt. Kern von SORA ist die Einordnung des geplanten UAS Einsatzes in eines von sechs Level, welche mit Anforderungen an den Betreiber, die Crew und das UAS selbst korrelieren.

Innerhalb des DLR Projekts ALAADy, für Automated Low Altitude Air Delivery, wird ein niedrig fliegendes UAS mit einer Tonne Nutzlast konzeptioniert, das weite Strecken zurücklegen können soll. Perspektivisch soll das ALAADy-Konzept in der EASA Kategorie *Specific* zum Einsatz kommen, welches ein Risiko Assessment nach SORA notwendig macht.
Je nach konkretem Einsatzszenario kann die Einstufung von ALAADy in eines der sechs Level variieren, mit unterschiedlichen Anforderungen an das UAS als Resultat. Ein Ziel innerhalb von ALAADy ist die Umsetzung eines möglichst kostenneutralen Konzepts, welches genau auf die regulativen Anforderungen zugeschnitten ist. Daher sollen innerhalb dieser Arbeit basierend auf den Anforderungen des SORA innerhalb der *Specific* Kategorie Vorschläge für geeignete Systemarchitekturen entwickelt werden. Diese sollen anschließend diskutiert und auf ihre Unterschiede hin untersucht werden. Um dem kostengünstigen Ansatz innerhalb das ALAADy Konzepts Rechnung zu tragen soll abschließend eine qualitative Abschätzung zu den erwarteten Umsetzungskosten für die Architekturvorschläge erfolgen.

Arbeitsschritte:

1) Einarbeiten in das DLR Projekt ALAADy bzw. in die Regulierung von UAS in der Kategorie *Specifc* und in SORA als zugrunde liegendes Risikoassessment.
2) Literaturrecherche und einarbeiten in gängige UAS Systemarchitekturen
3) Erarbeiten von auf dem ALAADy-Konzept basierenden Systemarchitekturen, welche den einzelnen Level in SORA gerecht werden.
4) Qualitative Abschätzung des Umsetzungsaufwands der erarbeiteten Systemarchitekturen
5) Dokumentation entsprechend der Vorgaben für Studienarbeiten der TU Braunschweig

Literaturvorschläge:
[1] JARUS guidelines on Specific Operations Risk Assessment (SORA)

Name des Studierenden: Daniel Rothe
Betreuer seitens DLR:
M.Sc. Florian Nikodem, Institut für Flugsystemtechnik, Abt. Sichere Systeme und Systems Engineering

Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

Date, Signature

Abstract

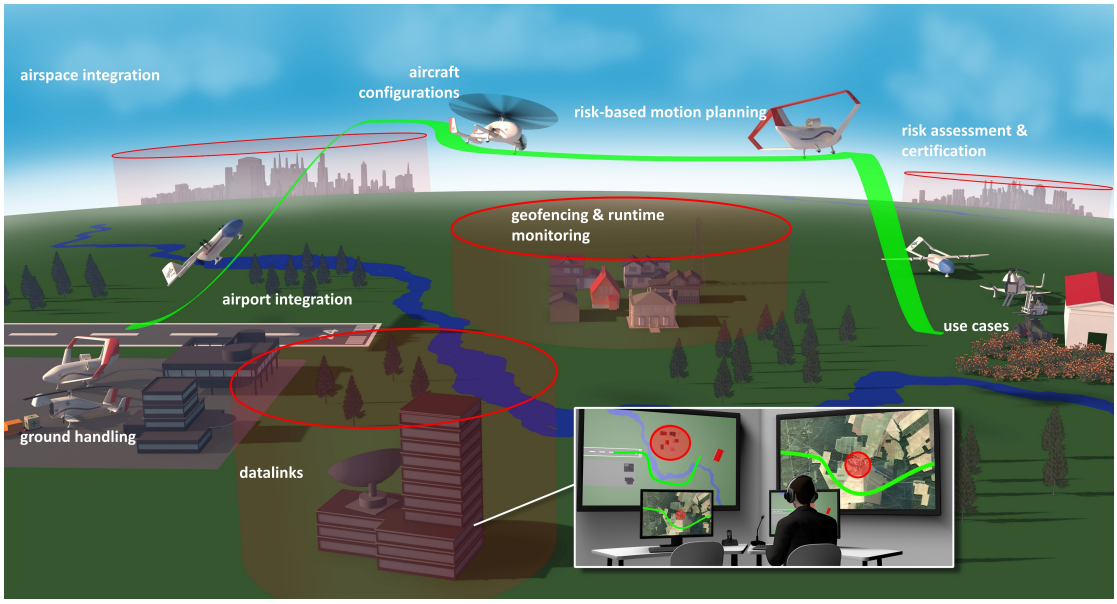
This Work develops a set of high-level system architectures for an Unmanned Aircraft System (UAS) for the low altitude transport of a 1 ton payload within the Automated Low Altitude Air Delivery (ALAADy) project. These architectures are further analyzed regarding their development effort. Based on the Specific Operation Risk Assessment [1] (SORA) as Acceptable Means of Comliance (AMC) for the specific category of the new European Union (EU) regulation for UAS, requirements are derived and processed into the architectures. An architecture for a certified system is developed for comparison as well. Overall, four major architectures are found. Within SORA, regarding the use case of a large cargo drone, only flights over sparsely populated areas are possible. Consequently, for flights over populated areas a certified system is necessary. Requirements in SORA are based on the risk which can be modified by mitigations. Therefore, different levels of requirements have to be used for the same mission depending on used mitigations. Within the analysis of the development effort a nondimensional relative effort factor is found. As a result, an ALAADy mission within SORA with less mitigations and sophisticated requirements has little difference to a certified system. Furthermore there is a gap found between two adjacent requirement levels. The development effort ranges from the least demanding to the most demanding architecture in half an order of magnitude.

Contents

1 Introduction

1.1. Motivation

Within the last years effort was shown in projects of Amazon, DHL, UPS and others to develop concepts of Unmanned Aircraft System (UAS) for transportation purposes. The German Aerospace Center, Deutsches Zentrum für Luft- und Raumfahrt (DLR) also works on transportation concepts with significantly increased payload capabilities within the Automated Low Altitude Air Delivery (ALAADy) project since 2016. The project goal is to analyze the concept of a large cargo drone regarding feasibility and economical issues. A special focus was taken on operational aspects and safety, the system architecture and necessary algorithms for realization. Multiple concepts were analyzed with different simulations including airspace simulations, system simulations and economical studies. Further tasks were the airspace integration concept, ground handling aspects of a large cargo drone, new propulsion concepts and a monitoring system for safe operation. Additionally, a prototype based on a commercial gyrocopter was built to gain operational experience. An illustration of the tasks included in an ALAADy mission is shown in figure 1.1.



Source: [2]

Figure 1.1.: Illustration of tasks included in an ALAADy mission.

The three developed configurations aim to transport medium-size payloads in an automated vehicle which has short take off and landing capabilities for flexible operational scenarios. The flight shall be conducted in very low level to avoid manned aviation and be able to fly around populated ar-

eas for safety reasons. For economical reasons the solutions found shall not be significantly pricier than a transport on road but much faster. A big impact on the economy of the concepts is given by the system architecture which has to satisfy the regulatory framework.
For example, a use-case found is the transport of spare parts for agricultural machines. When having a malfuntion during a harvesting operation, it is necessary to replace the faulty parts as fast as possible. An ALAADy mission could fly the needed parts directly to the field of the inoperative machine. Operation during humanitarian aid activity was considered as well.
Within the project this work focusses on the development and effort analysis of a set of system architectures which fulfill different regulatory levels. The different levels evolve from the Specific Operation Risk Assessment [1] (SORA) as an Acceptable Means of Comliance (AMC) for the specific category of the new European Union (EU) regulation for UAS. A comparison with a certified system is given as well.
The different architectures result in different economic characteristics. First of all the development and operating costs differ. Furthermore, the reliability varies and even the feasibility of a mission can be dependent on the resulting requirements. The developed architectures and the effort analysis shall contribute to find the best economic approach for the intended operation. This work focusses on technical issues and does not cover an operational perspective. A first estimation on the development effort for the architectures is given to find tendencies which can be further considered in future work.

1.2. Aircraft Configurations

Within the ALAADy project multiple concepts were chosen for a closer analysis. Different configurations were developed by identifying auspicious aircraft configurations in the context of the use-cases found. A market analysis generated operational scenarios of which requirements could be derived. Following, three specific configurations were designed conceptually to be further analyzed in flight performance, feasibility and inherent safety properties.
The selection of the configurations concludes with a *Twin Boom*, a *Box Wing* and a *Gyrocopter Configuration*. Renderings of the configurations are shown in figures 1.2, 1.3 and 1.4. These configurations have important characteristics for this work which are summarized in the following. All vehicles have a payload mass of 1 ton. The total mass of the configurations differs within an insignificant range for this study and can be assumed to be about 2.5 tons. The cruise speed is 200 km/h for all configurations. The flight altitude shall be below 150 m. The range for an ALAADy mission shall be up to 600 km. The aerodynamic steering is conducted by actuating aerodynamic control surfaces respectively a rotor tilt for the *Gyrocopter*. The flight can immediately be ended by a parachute ejection for the *Twin Boom* and *Box Wing Configuration* or an autorotation landing for the *Gyrocopter*. All configurations have multiple engines.

Source: [2]

Figure 1.2.: Rendering of the *Twin Boom Configuration*.

Source: [2]

Figure 1.3.: Rendering of the *Box Wing Configuration*.

Source: [2]

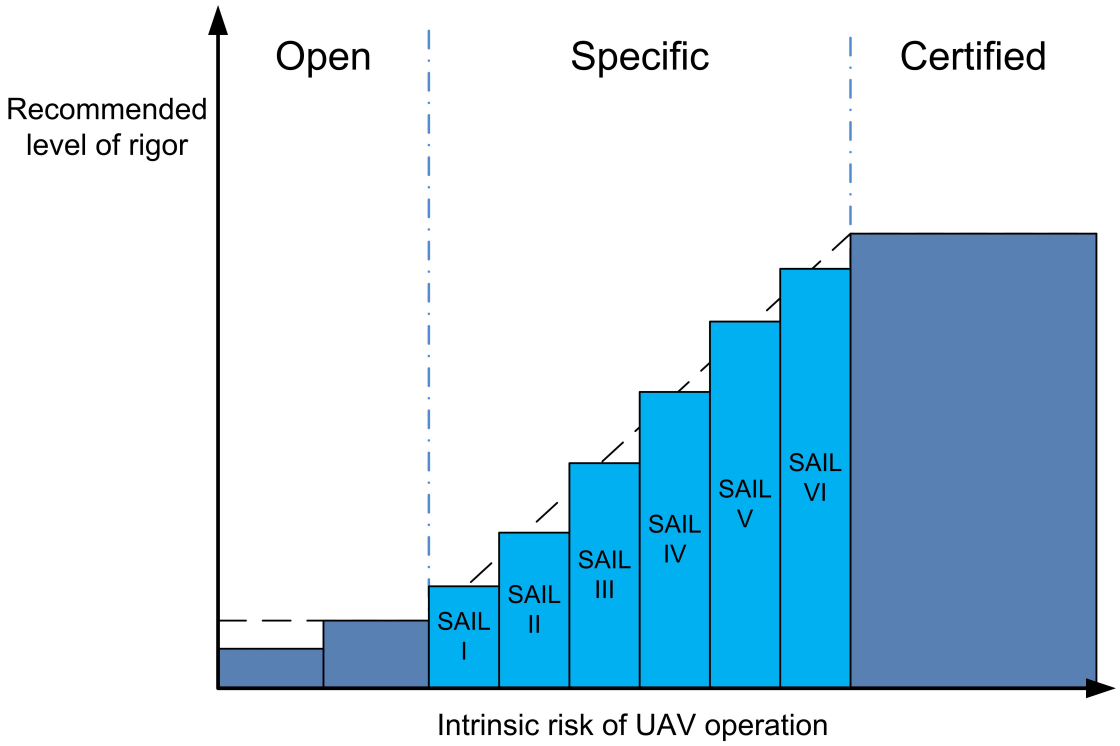
Figure 1.4.: Rendering of the *Gyrocopter Configuration*.

1.3. Structure

The structure of the remaining sections is as follows: First, in section 2 the legal demands are outlined and the resulting technical requirements are derived. In section 3 important decisions for the structure of the architectures are made. Section 4 conducts a hazard assessment, sets up the architecture and analyzes the development effort. Finally, a perspective on future work and a conclusion is given in section 5.

2 Regulatory Framework

In 2019, the country-specific regulations on the operation of UAS were replaced by the Commission Implementing Regulation (EU) 2019/947 [3] on the rules and procedures for the operation of unmanned aircraft which will entry into force in July 2020. To cover future developments this regulation was taken as basis of the further work.
In the regulation three categories for UAS are defined: open, specific and certified. The open category allows nonhazardous operations to be conducted without further oversight like flights for private uses with e.g. toy drones. Flights with a high damage potential for people or objects like the operation of heavy aircraft or operation in controlled airspace will fall into the certified category. A transition between these two categories is given with the specific category. This category aims to rise the level of requirements for a safe operation according to the intrinsic risk of the intended operation. This stepwise approach is visualized in figure 2.1.



Source: [4]

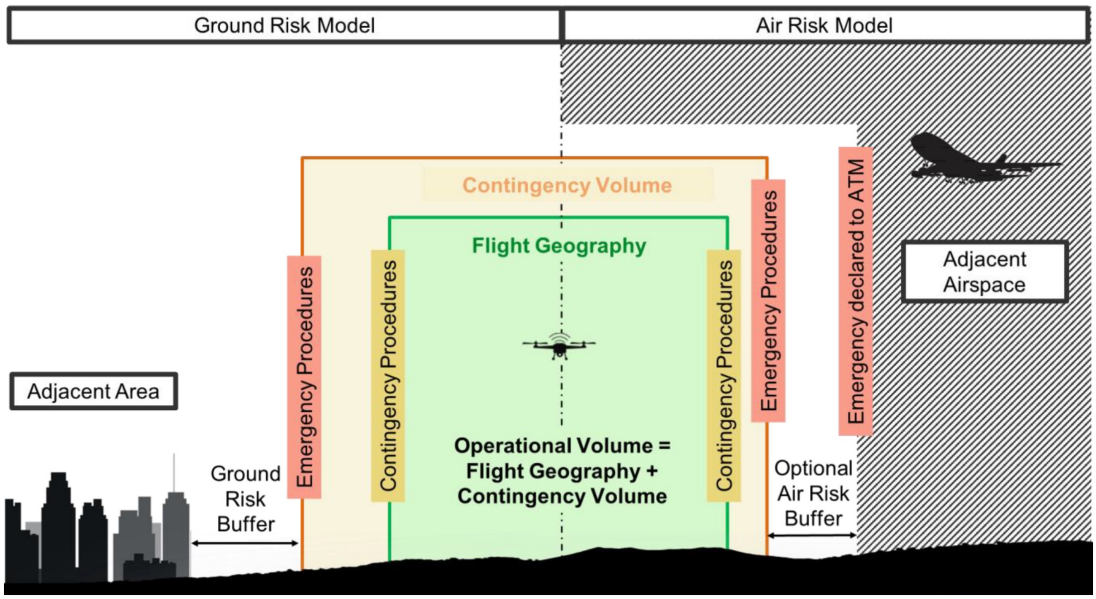
Figure 2.1.: Visualization of the stepwise approach within Regulation 2019/947.

Due to the size of the ALAADy configurations, the missions will not fit the conditions for an open operation. It is the goal of the ALAADy project not to fall into the certified category. Therefore, a

risk assessment is conducted with SORA to fit into the specific category. It is shown in section 2.2 that a flight over sparsely populated areas is in the scope of SORA. Flights over populated areas are out of scope of SORA. Due to the fact that ALAADy missions focus on flights over sparsely populated areas the following legal demands also focus on SORA. Furthermore, the requirements dictated by SORA are summarized. The information given in this section refers to SORA 2.0 [1]. A detailed set of requirements for certified UAS is not available yet. The approach to model the certified operation is described in section 4.2.

2.1. SORA Outline

SORA aims to reduce the risk of an unmanned flight operation by evaluating the severity of risks and giving instructions to reduce the probability of failure conditions happening in a sequence of steps. This is done by categorizing the risk into a Ground Risk Class (GRC) and an Air Risk Class (ARC). Both risk classes are found by defining an initial risk class and applying mitigations.
A semantic model which is visualized in figure 2.2 is used to describe the operation: The flight is conducted within a *Flight Geography*. It is surrounded by an optional *Contingency Volume* to apply *Contingency Procedures*. *Flight Geography* and *Contingency Volume* form the *Operational Volume*. The ground area around the *Operational Volume* is the *Ground Risk Buffer*, which has to be at least as wide as the flight altitude. Volumes are generally understood as a 2.5D-volume as a ground area combined with altitude information.



Source: [1]

Figure 2.2.: Visualization of the semantic model used.

In Step #1 of SORA, the relevant information has to be gathered in a concept of operation description. In Step #2, the initial GRC is determined by the vehicle characteristics of mass or impact energy, the overflown areas and whether the vehicle is flown in Visual Line of Sight (VLOS) or Beyond Visual Line of Sight (BVLOS). The GRC is scored by a positive integer which rises with the intrinsic risk. The value can be read from table 2.1 according the vehicle and mission characteristics.

Table 2.1.: Intrinsic GRC determination. Source: [1].

	Intrinsic UAS Ground Risk Class (GRC)			
Max UAS characteristics dimension	1 m	3 m	8 m	>8 m
Typical kinetic energy expected	<700 J	<34 kJ	<1084 kJ	>1084 kJ
Operational scenarios				
VLOS/BVLOS over controlled ground area	1	2	3	4
VLOS in sparsely populated environment	2	3	4	5
BVLOS in sparsely populated environment	3	4	5	6
VLOS in populated environment	4	5	6	8
BVLOS in populated environment	5	6	8	10
VLOS over gathering of people	7	-	-	-
BVLOS over gathering of people	8	-	-	-

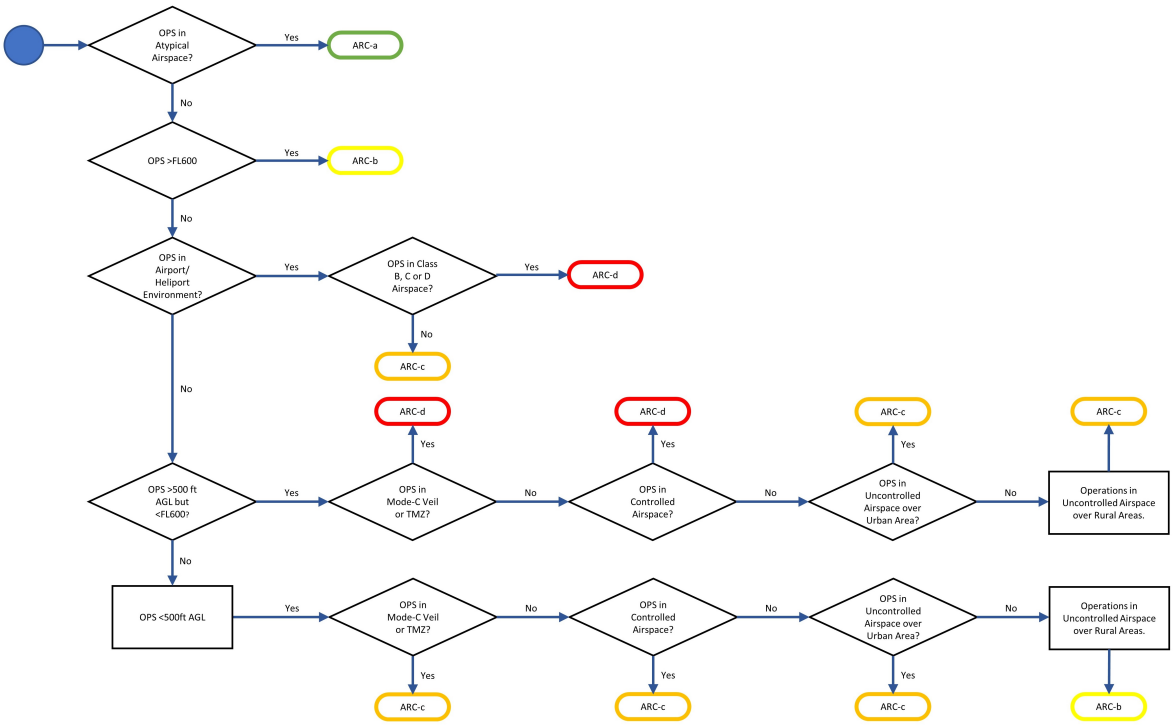
In Step #3, there are three mitigations which can be applied to lower the GRC. They cover the reduction of the number of people at risk, the reduction of the impact dynamics and the emergency response. All mitigations can be applied in different levels.
The M1 mitigation can be applied when there are efforts intended to reduce the number of people at risk. Therefore, it has to be shown that the actual number of people at risk is lower than initially assumed for the overflown area. There are no quantitative requirements given which makes it hard to foresee what is considered as a sufficient reduction of people at risk. However, there can be subtracted up to 4 points with this mitigation. Therefore, it is assumable that this mitigation shall cover e.g. operations with small drones over houses, where most of the people are sheltered against the operation by being inside or an operation above an industrial area beyond operating hours, where almost nobody is inside the covered area.
With mitigation M2 the reduction of effects of a ground impact are covered. For a medium level of robustness it has to be shown that the risk of fatalities nearby a ground impact are significantly reduced. For a high level of robustness it has to be shown that it is highly unlikely that a fatality can occur. A method to apply this mitigation could be the use of a parachute.

Mitigation M3 can be used when there is an Emergency Response Plan (ERP) available which reduces the post impact hazards.
The change in GRC according to the level of applied mitigation is shown in table 2.2.

Table 2.2.: Mitigations for final GRC determination. Source: [1].

		Robustness		
Mitigation sequence	**Mitigation for ground risk**	Low/None	Medium	High
1	M1 - Strategic mitigations for ground risk	0: None -1: Low	-2	-4
2	M2 - Effects of ground impact are reduced	0	-1	-2
3	M3 - An Emergency Response Plan (ERP) is in place, operator validated and effective	1	0	-1

The initial Air Risk Class (ARC) is found by the characteristics of the used airspace in Step #4. The ARC is described with a letter from a to d. ARC-a is an atypical airspace, which means e.g. a restricted airspace. ARC-d covers highly frequented airspaces like airfield control zones. The method to determine the ARC is shown in figure 2.3.



Source: [1]

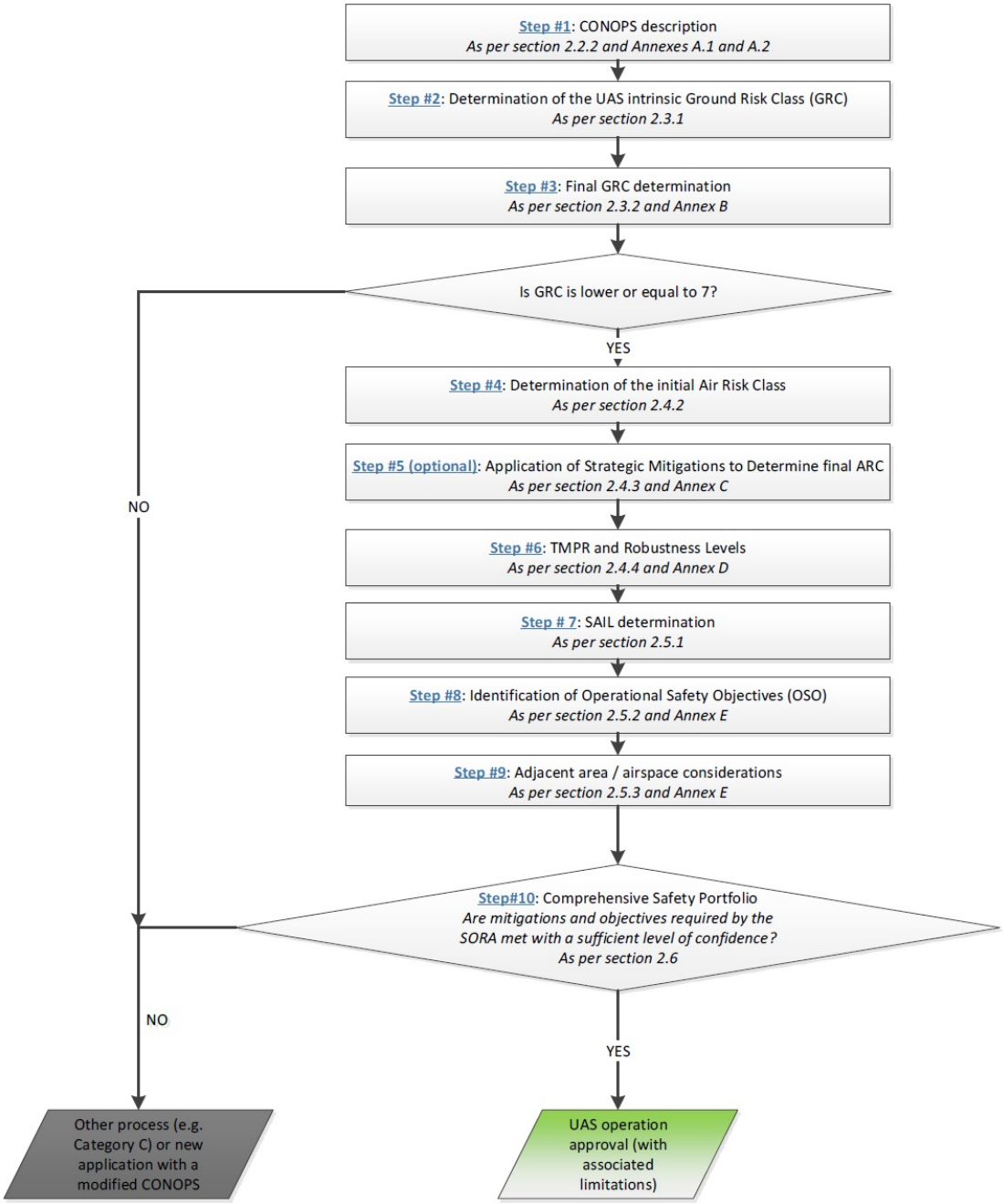
Figure 2.3.: Possible ARCs.

It is possible to reduce the ARC by applying a strategic mitigation in Step #5. In this mitigation it has to be shown that the used airspace is less frequented than generally assumed for this type of airspace. Resulting from the final ARC in Step #6, Tactical Air Risk Mitigation (TARM) have to be applied to lower the probability of a midair collision. These cover different robustness levels of detect and avoid capabilities which are mandatory.
In Step #7, the two risk classes are summarized into one of six Specific Assurance and Integrity Levels (SAIL). Table 2.3 shows the determination of the SAIL.

Table 2.3.: SAIL determination. Source: [1].

Final GRC	**Residual ARC**			
	a	b	c	d
<=2	I	II	IV	VI
3	II	II	IV	VI
4	III	III	IV	VI
5	IV	IV	IV	VI
6	V	V	V	VI
7	VI	VI	VI	VI
>7	Certified			

Resulting from the SAIL multiple Operational Safety Objectives (OSO) have to be met which is described with Step #8. OSO exist on three different robustness levels: low, medium and high. Which of the levels has to be used is depending on the SAIL. Some OSO do not have to be considered for low SAIL.
Additionally, Step #9 defines criteria to avoid endangering adjacent areas. Finally, the compliance with the requirements has to be shown in Step #10.
A summary of the SORA process is given in figure 2.4.



Source: [1]

Figure 2.4.: Summary of the SORA process.

2.2. Possible Scenarios

SORA enables multiple approaches for a project by varying the mission scenario or mitigations. The following section shows which possibilities are given by conducting a risk assessment according to the SORA process.
The GRC is evaluated by overflown areas and vehicle characteristics. The ALAADy configurations are classified into the most dangerous vehicle class because of the possible impact energy resulting from the mass of about 2.5 tons. In addition, all flights will be conducted Beyond Visual Line of Sight (BVLOS). Still, two different initial GRCs can be set for ALAADy missions depending on flying over populated areas or avoiding them. The resulting numbers evolve from table 2.1 and are 6 for a flight over sparsely populated areas and 10 for flights over populated areas.
Within the context of the ALAADy missions some mitigations can be used. By applying the three mitigations within their possible range the initial GRC changes to the final values. The change numbers result from table 2.2.
For using the M1 mitigation, when flying an ALAADy mission over sparsely populated areas, it would have to be shown that there are practically no individuals overflown. Therfore, the whole area overflown would have to be monitored which is not possible on a ALAADy mission which is up to 600 km long. When flying over populated areas the argument of sheltered people cannot be used due to the mass of an ALAADy vehicle which would easily break a normal roof. Avoiding populated areas would result in a flight over sparsely populated areas which is already covered with the two possibilities in the intrinsic GRC. Therefore, the M1 mitigation is not used.
By using a method to have a controlled crash with minimum velocity, mitigation M2 can be applied on a medium level. A high level cannot be reached because it would have to be shown that a fatality can most likely not occur. This is not possible because the mass of the vehicle would crush a person even if landed with infinitisemal low velocity and a soft underside with airbags. However, this mitigation does not need to be used which leads to a reduction of the GRC of zero or one points.
By using no ERP the M3 mitigitation would result in an additional GRC point. But also the high level of robustness seems to be reachable when using an emergency sound system onboard combined with a controlled crash with minimum velocity to satisfy the requirement of reasonably expecting no fatalities in case of a crash, at least when not flying over populated areas. The high level of robustness would result in a reduction of one point.
The final values give a range between best and worst cases depending on the applied mitigations and are presented in table 2.4.

Table 2.4.: Possible GRC depending on mission scenario and applied mitigations.

Value	**Sparsely Populated**	**Populated**
Initial GRC	6	10
Highest Change by mitigations	+1	
Lowest Change by mitigations	-2	
Highest possible GRC	7	11
Lowest possible GRC	4	8

SORA can only be applied when the final GRC is 7 or lower. If this requirement is not met, a certification needs to be applied. Therefore, flights over populated areas are out of the SORA scope. The ARC is evaluated by the characteristics of the used airspace. ARC-a is reserved for restrictive airspace. Because ALAADy missions are planned to use nonrestrictive airspace the ARC can range from b, when avoiding frequented airspace, up to d, when using public airfields and their control zones.
With the use of a strategic mitigation it would be possible to lower the ARC. However, a reduction down to ARC-a would not be possible. The required encounter rate would not be reached because of possible off-field landings of gliders or emergency operations of rescue helicopters. The range of ARC-b to -d is already studied so any other reduction does not need to be considered.
The SAIL evolves from GRC and ARC by table 2.5. The possible SAIL are marked green and reach from 3 to 6.

Table 2.5.: SAIL determination. The green marked SAIL are the possible range within SORA for ALAADy missions. Modified from [1]

Final GRC	**Residual ARC**			
	a	b	c	d
<=2	I	II	IV	VI
3	II	II	IV	VI
4	III	III	IV	VI
5	IV	IV	IV	VI
6	V	V	V	VI
7	VI	VI	VI	VI
>7	Certified			

2.3. Technical Requirements

Technical requirements evolve from three sections within SORA. These are Step #9 in the main part, Annex D with requirements for TARM and Annex E with OSO.

Step #9 defines requirements for containment. The resulting safety requirements which affect the system architecture are:

- No probable failure of the UAS or any external system supporting the operation shall lead to operation outside of the *Operational Volume*.

Aditionally, the following requirements have to be considered when there are gatherings of people in the adjacent area:

- The probability of leaving the *Operational Volume* shall be less than 10^{-4}/Flight Hour (FH).
- No single failure of the UAS or any external system supporting the operation shall lead to operation outside of the *Ground Risk Buffer*.
- Software (SW) and Airborne Electronic Hardware (AEH) whose development error(s) could directly lead to operations outside of the *Ground Risk Buffer* shall be developed to an industry standard or methodology recognized as adequate by the competent authority.

According to the SORA terms a *Ground Risk Buffer* is a zone following the Operational Volume to protect adjacent areas of enhanced vulnerability. The width of the *Ground Risk Buffer* has to be at least the same number as the flight altitude. Due to the large *Flight Geography* and the possible range of the used vehicle, it is assumed that ALAADy missions will have to consider gatherings of people in adjacent areas. Therefore, the four requirements above will have to be applied.

Requirements for a Tactical Air Risk Mitigation (TARM) System (TARMS) are defined in Annex D of SORA. This mandatory mitigation defines capabilities of a detect and avoid system. For flights beyond visual line of sight each ARC has different requirements. The Annex gives recommendations for systems to be used, recommendations for agility and requirements for reaction times. For ARC-d a system meeting RTCA SC-228 or EUROCAE WG-105 Minimum Operational Performance Standards (MOPS)/ Minimum Aviation System Performance Standard (MASPS) or similar is required. Requirements for detection rate and reliability are given in table 2.6.

Table 2.6.: Requirements for TARMS from Annex D of [1] regarding detection and failure rate. Source: [1].

Value	**ARC-b**	**ARC-c**	**ARC-d**
Detection Rate	50%	90%	See RTCA SC-228 or EUROCAE WG-105 or similar
Failure Rate	$<10^{-2}$/FH	$<10^{-3}$/FH	$<10^{-5}$/FH

General requirements are OSO, provided by Annex E of SORA. Not all OSO contain technical requirements. The requirements which contain technical regulations are described below. Only the level of integrity is summarized because the level of assurance does not affect the system architecture. Still, the level of assurance can be important for the development effort. It is assumed that this influence is covered with the assigned Design Assurance Level (DAL). For closer details see Annex E of SORA.

- OSO #4: UAS developed to authority recognized design standards
- OSO #5: UAS is designed considering system safety and reliability
  - On a medium level of integrity a strategy is required to detect, alert and manage any malfunction or failure which would lead to a hazard.
  - On a high level of integrity given probabilities of different failure conditions need to be met.
- OSO #6: C3 link characteristics
  - This OSO prescribes that the link has to be appropriate for the mission and that it has to be monitorable. The used methodology in this work does not further process this requirement.
- OSO #10: Safe recovery from technical issue

- OSO #12: The UAS is designed to manage the deterioration of external systems supporting UAS operation
- OSO #10 and #12 are described commonly. They only apply when flying over populated areas. Therefore, it is not further considered.
- OSO #13: External services supporting UAS operations are adequate to the operation
  - This OSO prescribes that the external services have to be appropriate for the mission. The used methodology in this work does not further process this requirement.
- OSO #18: Automatic protection of the flight envelope from human errors
- OSO #19: Safe recovery from Human Error
- OSO #20: A Human Factors evaluation has been performed and the Human Machine Interface (HMI) found appropriate for the mission
  - This OSO prescribes that the HMI has to be appropriate for the mission. The used methodology in this work does not further process this requirement.
- OSO #24: UAS designed and qualified for adverse environmental conditions
  - This OSO prescribes that UAS has to be appropriate for the environmental conditions during the mission. The used methodology in this work does not further process this requirement.

The robustness level to be used is defined by the SAIL. The assignment is summarized in table 2.7.

Table 2.7.: Assignment of robustness Levels to SAIL according to [1].

Requirement	**SAIL III**	**SAIL IV**	**SAIL V**	**SAIL VI**	**certified**
Step#9	Required in general				SORA requirements not applicable
TARMS	Depending on ARC flown				
OSO #4	-	L	M	H	
OSO #5	L	M	H	H	
OSO #18	L	M	H	H	
OSO #19	L	M	M	H	

3 System Definition

The different system architectures are based on assumptions which are outlined in this section. The first section characterizes a Monitoring System which is indirectly suggested by SORA. Then general assumptions are described which the system architectures are derived from. Finally, the used system terms are defined.

3.1. Monitoring System

Step #9 in the SORA process dictates requirements to protect adjacent areas. A detailed description is found in section 2.3. Step #9 requires the UA to leave the *Operational Volume* just with a certain probability of 10^{-4}/FH. In addition no single failure is allowed for the UA to operate outside the *Ground Risk Buffer*. When aiming for a simple UAS without redundancy a possibility to satisfy these requirements is to implement a Monitoring System which is able to end the flight immediately by a controlled crash when certain criteria are violated. In case of ALAADy configurations, this flight termination shall be conducted by deactivating the propulsion system and triggering the Impact Dynamics Reduction System (IDRS) which is described in section 3.3. According to the SORA terms a flight termination is an emergency procedure and not an operation.
When using a Monitoring System there are two ways to fulfill the requirements by Step #9:

1. The Monitoring System terminates when leaving the *Contingency Volume*. The controlled crash is conducted inside the *Ground Risk Buffer*.
2. The Monitoring System terminates when leaving the officially defined *Flight Geography*. The controlled crash is conducted inside the *Contingency Volume*.

According to the SORA terms the *Operational Volume* consists of a *Flight Geography* where the mission is conducted normally and a *Contingency Volume* to apply *Contingency Procedures*. The size of the *Contingency Volume* is not prescribed in general.
Without substantiated evidence of the reliability of the pilot, the technical systems alone have to fulfill the requirements dictated by Step #9.
SORA does not require to adjust the size of the *Ground Risk Buffer* to the potential range of the vehicle in case of a termination. For own interest the *Ground Risk Buffer* should be carefully sized.
Variant 2 allows setting internal *Contingency Procedures* to prevent breaching the *Flight Geography* without terminating the flight.
The two variants are summarized in table 3.1.

Table 3.1.: Requirements for systems and mission depending on the used termination variant. "Flight System" can be interpreted as all systems excluding the monitoring system.

Subject	**Variant 1**	**Variant 2**
Verified failure rate for the Monitoring System	No requirement	$<10^{-4}$/FH (combined with Flight System)
Verified rate for failures that lead to operation outside the *Operational Volume* for the Flight System	$<10^{-4}$/FH	$<10^{-4}$/FH (combined with Monitoring System)
Size of *Ground Risk Buffer*	1 to 1 (reference: altitude)	1 to 1 (reference: altitude)
Size of *Contingency Volume*	No requirement	Depending on possible range after termination

The flight paths of the two variants are shown in figure 3.1. It can be seen, that Variant 1 allows for a larger *Flight Geography*.

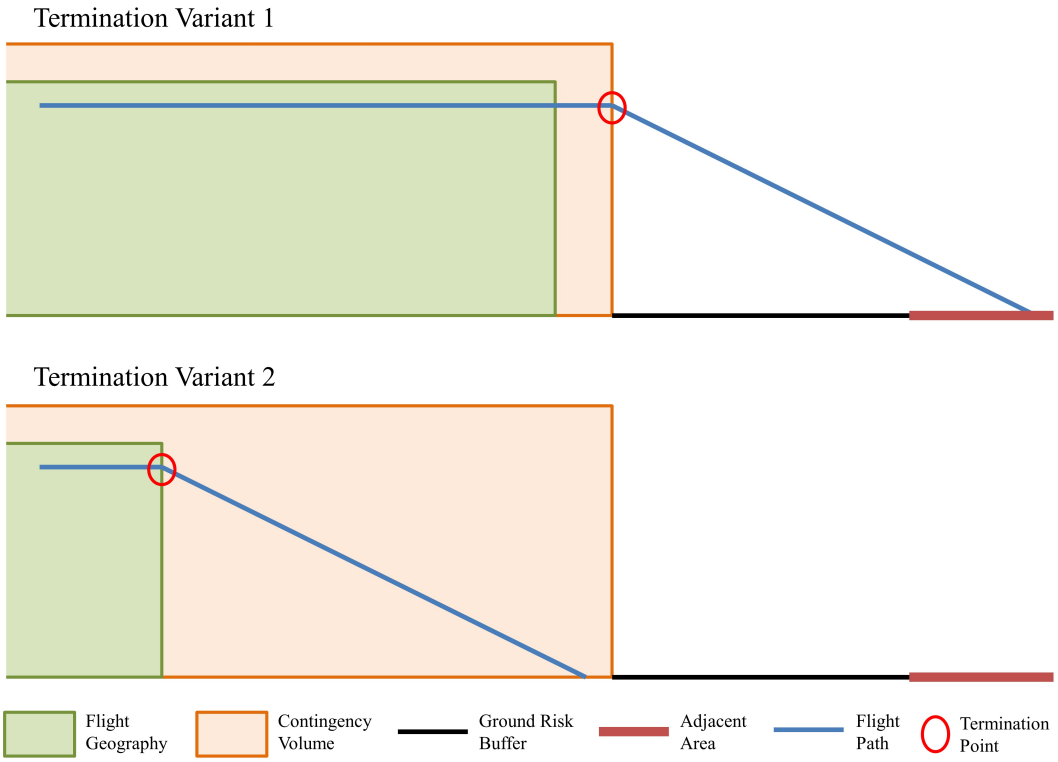


Figure 3.1.: Visualization of flight paths depending on the termination variant.

Both variants have a specific advantage. They are:

- Advantage Variant 1: Larger *Flight Geography*
- Advantage Variant 2: Lower complexity challenges due to decreased reliability requirements

The selection of one variant does not affect the system architecture but the effort to realize the system because of a changing DAL. Therefore, the effort of each Variant is evaluated in section 4.4.

3.2. General Assumptions

The setup of the system architectures follows general assumptions which are outlined in the following.
The ALAADy configurations differ in certain aspects like the principle of aerodynamic steering or the setup of the propulsion elements. The system architectures therefore are described on an abstract level to cover all configurations in one view. Consequently it is not possible to evaluate the configurations in this context.
It is assumed that redundant systems are much more expensive to develop than nonredundant systems. Within this work, redundancy is ment as independent systems and not only available multiple

times. Therefore, redundancies are only applied when necessary because of legal demands. Single failures are avoided by using a Monitoring System when possible.
Redundant systems are implemented when failure conditions need to be considered and a general failure in a system would lead to a failure condition which is hazardous or higher. The kind of necessary redundancy, like the number of components or dissimilarities, is not considered further. To reach the necessary reliability of components a DAL is allocated (DAL as defined in ARP4754A [5]). The DAL was developed for manned aviation and reaches from E to A. DAL E is used for systems with no safety effect while DAL A is used for systems which can cause catastrophic failures. For unmanned systems AMC RPAS.1309 [6] is an adaption which is used in this work. The different DAL cover different required processes to ensure reliable development of systems. The kind of necessary requirements, the development of standards, the review by third parties and the development sequence is defined and gets more sophisticated for higher DAL.
All Systems could cause a loss of the vehicle and shall be developed to a DAL of at least D. This shall be done independent of a lack of legal demands to ensure a minimum reliability of an ALAADy mission.
The difference of the requirements for SAIL V and VI is small. In the further processed requirements it covers only OSO #4 and #19. OSO #19 differs only in the level of assurance. The difference in OSO #4 is a soft description about the compliance with standards used. These differences are not further considered to reduce the complexity of this work. This leads to the simplification that there are no differences in the effort to develop a system for SAIL V or VI.
The solutions found generally try to describe the simplest architecture for a set of requirements. There is always the possibility to increase the complexity of an architecture for non-safety reasons.

3.3. Terms

To describe the system architectures independent of specific solutions, it is described on a logical level. The Terms used are defined in the following.

3.3.1. Central Computational Elements

CS – Communication System. Covers the elements in the UA to establish a C2 link and communication avionics like transponders. Communication avionics are commercially available. To focus on the systems which have to be developed for an ALAADy configuration, they are not further modelled.

FCS – Flight Control System. Is able to translate operator inputs and position, attitude and velocity information from the PFAS into steering commands. Operator inputs can be direct control or waypoints. It therefore covers an autopilot as well.

FCELS – Flight Control and Emergency Landing System. Contains a FCS with the additional capa-

bility of conducting an emergency landing and further emergency procedures to be able to operate over populated areas in a certified system.

FEHEP – Flight Envelope and Human Error Protection. Monitors steering commands to prevent the vehicle from exceeding certain limits by giving feedback to the FCS. Limits are for example maximum velocities or loads. It can also protect the vehicle from breaching the allowed *Flight Geography*. Satisfies OSO #18 and #19.

GS – Ground Station. Covers the elements to establish a C2 link on ground, interfaces for the operator and related computational elements.

Link – Connection between CS and GS.

MDS – Malfunction Detection System. Is able to monitor critical functions and elements of the vehicle. The feedback can be used by the FCS autonomously or the operator. Satisfies medium level of integrity of OSO #5.

PFAS – Position and Flight Condition Acquisition System. Gathers information like position, altitude, velocities and attitude.

TARMS – Tactical Air Risk Mitigation System. SORA requires Tactical Air Risk Mitigation (TARM) when flying an ARC-b or higher. A closer review of the requirements for the TARM can be found in section 2.3. Architectures on the same SAIL differ only in the required TARMS. Therefore, it is represented by the same block to reduce the number of visualized architectures. In the cost estimation the difference for each ARC is considered.

3.3.2. Actuation Elements

PAS – Primary Actuation Systems. For aerodynamic steering the actuation of flaps or rotors is necessary. The PAS cover the elements required for controlled flight.

SAS – Secondary Actuation Systems. SAS cover all actuated elements which are not necessarily needed for control of flight like drag flaps.

3.3.3. Propulsion Elements

FSS – Fuel Supply System. To propel the vehicle a supply of fuel is needed. This function is covered with the FSS. It covers the supply of internal combustion engines as well as fuel cells, if implemented in the configuration.

PS – Propulsion Systems. The aerodynamic lift generates drag which needs to be compensated by Propulsion Systems. The Propulsion Systems also enable the vehicle to lift off and climb. The ALAADy configurations generally have multiple propulsion systems. PS covers internal combustion engines and electrical engines, if implemented in the configuration. It is assumed that the engine will be bought. This component therefore focusses on the link between the control system and the

engine.

3.3.4. Other Elements

MS – Monitoring System. As described in section 3.1. The MS is completely independent regarding position and attitude acquisition to avoid common failures. If not independent in power supply the system has to be deployed when losing the power supply. Contains elements to calculate the validity of the flight state and the elements to bring the vehicle into the terminated flight state, e.g. a parachute. The Monitoring System is implemented to satisfy Step #9 for low SAIL.

IDRS – Impact Dynamics Reduction System. For ALAADy missions it is generally stated that a termination of the flight shall be possible. The responsible system can be triggered as an emergency procedure as described in chapter 6. For the *Box Wing* and *Twin Boom Configuration* the termination system relies on a parachute ejection. The *Gyrocopter Configuration* shall land in autorotation. In addition the Propulsion System is deactivated. These systems are modelled as an IDRS.

Power. Contains all elements to provide power in the UA. It also covers the supply of electrical engines, if implemented in the configuration.

4 System Variants

In this section the different system architectures are developed and analyzed. The system architectures are defined for each system variant found. The range of possible variants is defined by table 2.5 and if a Monitoring System is applied, the termination variant as described in section 3.1. In addition, a system architecture for a certified system is developed to give a comparison to high SAIL as well. The naming scheme for the architectures based on SORA includes the specific Assurance and Integrity Level, the Air Risk Class and, if applied, the Termination Variant (TV). An example is SAIL IV, ARC-b, TV 1.

4.1. Required Components

To perform a mission, most of the defined systems have to be implemented. There is either a Flight Control System (FCS) or a Flight Control and Emergency Landing System (FCELS). FCELS is only implemented in a certified system to be able to apply autonomous emergency procedures to avoid crashing into populated areas. Flight Envelope and Human Error Protection (FEHEP) and Malfunction Detection System (MDS) are implemented depending on the SORA requirement. FEHEP is required from SAIL III on and therefore for all variants. MDS is required from SAIL IV on.
A Monitoring System (MS) is only implemented for SAIL III and IV. From SAIL V on OSO #5 dictates that a loss of the vehicle is a hazardous failure condition and must not occur with a higher probability than 10^{-7}/FH as described more detailed in section 4.2. This, however, is a stricter requirement than not to leave the *Operational Volume* with a probability of 10^{-4}/FH dictated by Step #9. Because MS is implemented to avoid redundancies in the first place and with OSO #5 on high robustness level redundancies are necessary anyway, MS is not implemented for higher SAIL and a certified system.
The Impact Dynamics Reduction System (IDRS) is not implemented for a certified system, because failure is not an option.
A summary of these information is listed in table 4.1.

Table 4.1.: Implemented Components for different architectures.

Component	SAIL III, ARC-b, TV 1/2	SAIL IV, ARC-b/c, TV 1/2	SAIL V or VI, ARC-b/c/d	certified
CS	√	√	√	√
FCS	√	√	√	
FCELS				√
FEHEP	√	√	√	√
GS	√	√	√	√
Link	√	√	√	√
MDS		√	√	√
PFAS	√	√	√	√
TARMS	√	√	√	√
PAS	√	√	√	√
SAS	√	√	√	√
FSS	√	√	√	√
PS	√	√	√	√
MS	√	√		
IDRS	√	√	√	
Power	√	√	√	√

4.2. Hazard Assessments

A hazard assessment is conducted to find the DAL and required redundancies of the components. The established fault trees follow ARP4761 [7]. Conseqently, the gates seen in the following figures are AND-Gates. Description of outputs are given in boxes. An event which will happen and is external to the system under analysis, is shown in a pentagon. The events in a diagonal square are not further developed, because more details would not improve the outcome. A hexagon describes that the input will lead to described output, if a conditional event is present. The conditional event is shown in the box with rounded edges.
It was necessary to simplify the process which leads to inaccuracies. However, this gives a rough first estimation to compare multiple variants. The target numbers evolve from Step #9 and OSO #5 on high level robustness. Step #9 is closer described in section 2.3. These requirements are only applied to the ground risk, because it is assumed that as long as the vehicle does not leave the *Operational Volume* the air risk is already considered within the TARM. Leaving the *Operational Volume* is covered with Step #9 though.
For the SAIL III and IV variants, OSO #5 on high level of robustness does not need to be considered and only Step #9 is relevant. In SAIL III and IV a monitoring system is to be used as described in section 3.1. Therefore, only the requirement of not leaving the *Operational Volume* with a probability of 10^{-4}/FH is evaluated here.
For each of the termination variants as listed in table 3.1 a different fault tree has to be prepared. Without substantiated evidence of the reliability of the pilot, the technical systems alone have to fulfill the requirements dictated by Step #9. Therefore, it is assumed for both fault trees that the adjusted flight path will leave the *Operational Volume* and the *Ground Risk Buffer*.
Figure 4.1 shows the related fault tree for termination variant 1 when a termination is performed just before leaving the *Operational Volume*.

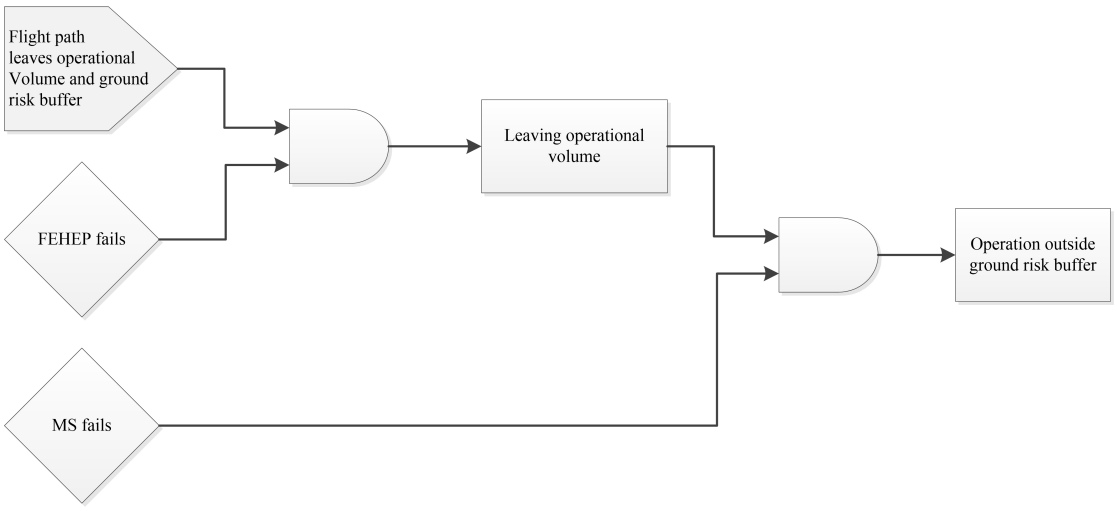


Figure 4.1.: Fault tree for SAIL III or IV, TV 1.

It can be seen that the FEHEP component is responsible for preventing the leaving of the *Opera-*

tional Volume. Therefore, it has to fulfill the reliability of 10^{-4}/FH. It is assumed that as consequence the FEHEP and all components that could interfere have to be developed as DAL C. All other systems could cause a loss of the vehicle and therefore are developed as DAL D for own interest. No outage of any component can directly lead to a violation of the Step #9 requirements. Therefore, no redundancies are mandatory. The results are summarized in table 4.2.

Table 4.2.: Required DAL and redundancies for SAIL III or IV, TV 1 architectures.

Component	**DAL**	**Redundancy**
CS	C	No
FCS	C	No
FEHEP	C	No
GS	C	No
Link	C	No
MDS (only SAIL IV)	D	No
PFAS	C	No
TARMS	Depending on ARC flown	
PAS	D	No
SAS	D	No
FSS	D	No
PS	D	No
MS	D	No
IDRS	D	No
Power	D	No

The fault tree for termination variant 2 is similar to that of termination variant 1 and can be seen in figure 4.2. Here, the termination occurs before leaving the *Operational Volume.*

In this variant the FEHEP component and the monitoring system are responsible for preventing the leaving of the *Operational Volume.* Thus, the two systems combined have to fulfill the reliability

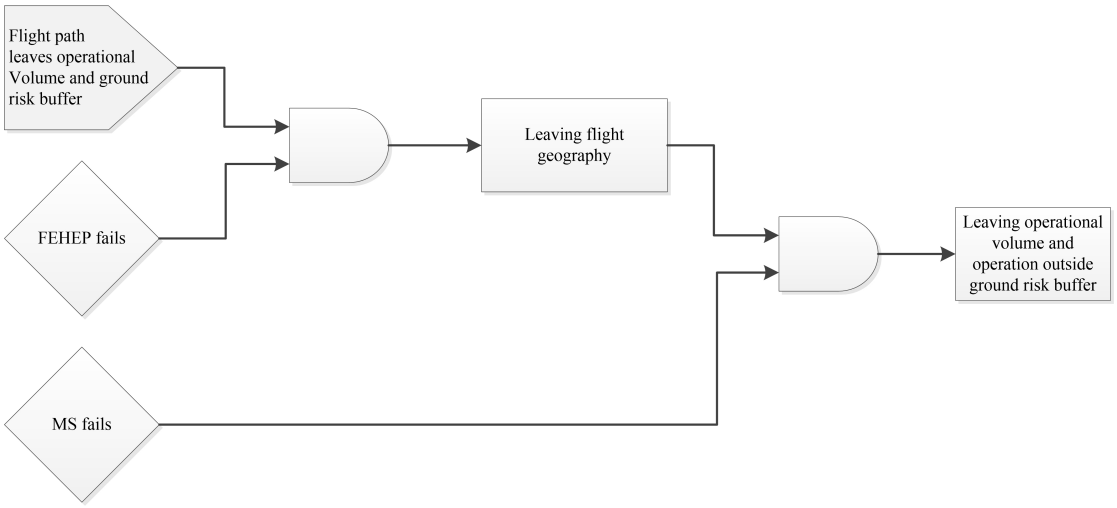


Figure 4.2.: Fault tree for SAIL III or IV, TV 2.

of 10^{-4}/FH. As consequence, the FEHEP and all components that could interfere as well as the monitoring system have to be developed as DAL D. All other systems could cause a loss of the vehicle and therefore are developed as DAL D as well for own interest. No outage of any component can directly lead to a violation of the Step #9 requirements. Therefore, no redundancies are mandatory. The results are summarized in table 4.3.

Table 4.3.: Required DAL and redundancies for SAIL III or IV, TV 2 architectures.

Component	**DAL**	**Redundancy**
CS	D	No
FCS	D	No
FEHEP	D	No
GS	D	No
Link	D	No
MDS (only SAIL IV)	D	No
PFAS	D	No
TARMS	Depending on ARC flown	
PAS	D	No
SAS	D	No
FSS	D	No
PS	D	No
MS	D	No
IDRS	D	No
Power	D	No

For SAIL V or VI Step #9 and OSO #5 on a high level of robustness have to be considered. OSO #5 requires in high level of integrity:

- Major Failure Conditions are not more frequent than Remote
- Hazardous Failure Conditions are not more frequent than Extremely Remote
- Catastrophic Failure Conditions are not more frequent than Extremely Improbable

Specific definitions of the Terms are given in AMC RPAS.1309 [6] with a recap in the following. A malfunction of any component with exception of the IDRS is considered as a major failure condition. A loss of the vehicle or an emergency landing is considered as a hazardous failure condition. One or more fatalities are considered as a catastrophic failure condition. The allowed probabilities for the given failure conditions evolving from a multi reciprocating or turbine engine of less than 6000 lbs with complexity level II are shown in table 4.4.

Table 4.4.: Required quantitative failure probability and DAL for different failure conditions from AMC RPAS.1309 [6].

Failure Condition	**Allowable Quantative Probability**	**Required Design Assurance Level**
Major	$<10^{-5}$/FH	C
Hazardous	$<10^{-7}$/FH	B
Catastrophic	$<10^{-8}$/FH	B

Leaving the *Operational Volume* is considered to be a hazardous failure condition, because it will likely result in an emergency landing or the loss of the vehicle. The operation outside the *Ground Risk Buffer* is considered to be a catastrophic failure condition, because it is likely that an emergency landing or a crash will result in fatalities here. As a consequence, the requirements of Step #9 are exceeded by the requirements resulting from OSO #5 on a high level of robustness and are not further considered.
The fault tree of a SAIL V or VI architecture can be seen in figure 4.3.
Most systems can cause catastrophic failure conditions and therefore are DAL B. An outage could lead to a failure condition which is at least major. Consequently, redundancies are applied to meet the quantitative probabilities. However, some exceptions can be made.
DAL B is necessary for the MDS, because of possible interferences with other systems. A redundancy does not seem to be necessary because a loss of this component would just result in a safety landing at the next possibility which is not a major failure condition.
The SAS cannot lead to hazardous failure conditions and therefore are DAL C without redundancy. However, in a specific system this could change for certain components like a retractable gear whose outage in the retracted position could cause a loss of the vehicle.
The PS is assumed to base on commercial off the shelf engines. Because multiple engines are implemented the PS does not require a redundancy for each engine.

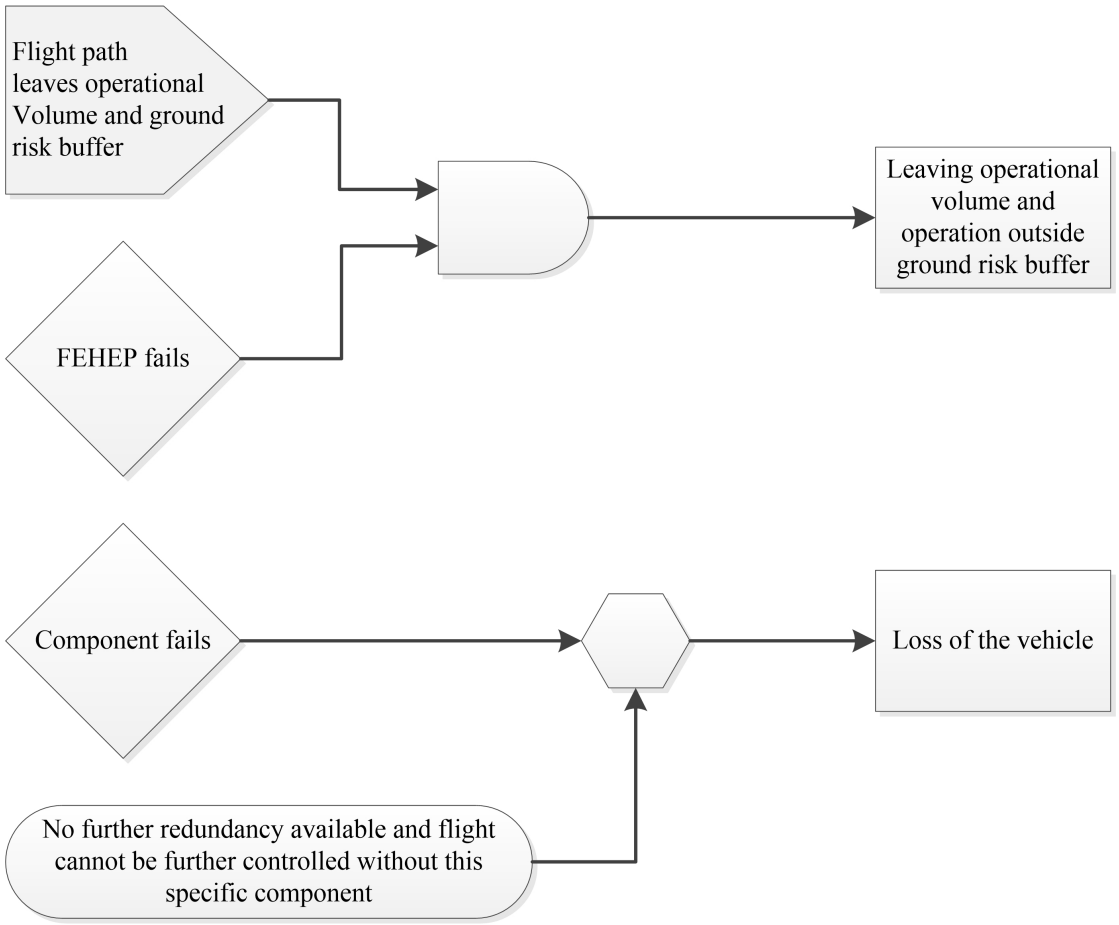


Figure 4.3.: Fault tree for SAIL V or VI.

The IDRS does not lead to major failure conditions so the minimum DAL of D without redundancy is assumed. However, this decision needs to be closer reviewed if the IDRS is able disturb the flight significantly e.g. with the ejection of a parachute.
ARP4754A [5] allows to reduce the DAL, when having independent redundancies. So the DAL B systems could be reduced to DAL C systems, when having independent redundancy anyway. However, it was not further examined, in which cases interdependencies would forbid the use of this possibility, so it was not used within this work. Future analysis should consider this option.
A summary of the results can be seen in table 4.5.

Table 4.5.: Required DAL and redundancies for SAIL V or VI architectures.

Component	DAL	Redundancy
CS	B	Yes
FCS	B	Yes
FEHEP	B	Yes
GS	B	Yes
Link	B	Yes
MDS	B	No
PFAS	B	Yes
TARMS	Depending on ARC flown	
PAS	B	Yes
SAS	C	No
FSS	B	Yes
PS	B	No
IDRS	D	No
Power	B	Yes

Requirements for a certified operation are not available yet. To find a comparative architecture, assumptions were made on how a certified system will be structured.
For SAIL V and VI, OSO #5 dictates that certain failure probabilities have to be met for certain failure conditions. These derive from the AMC RPAS.1309 [6] which also applies for the certified category. It is assumed that the development effort mainly evolves from the process to attain required reliabilities. When the same failure rates have to be met, equal processes are necessary which build on similar requirements. Therefore, the evolving architecture for SAIL V or VI is taken with the highest ARC to find the certified architecture. Some modifications have to be made to be applicable for flights over populated environments. These cover the Flight Control System that should be able to conduct emergency landings and the possibility to terminate a flight is discarded.
The differing systems used result in table 4.6.

Table 4.6.: Required DAL and redundancies for a certified system architecture.

Component	DAL	Redundancy
CS	B	Yes
FCELS	B	Yes
FEHEP	B	Yes
GS	B	Yes
Link	B	Yes
MDS	B	No
PFAS	B	Yes
TARMS-d	C	Yes
PAS	B	Yes
SAS	C	No
FSS	B	Yes
PS	B	No
Power	B	Yes

The DAL and Redundancies for the TARMS evolve from Annex D which is closer described in section 2.3. The results are listed in table 4.7. For TARMS-b no DAL is necessary. This component can probably not result in a loss of the vehicle. Therefore, no DAL is applied for reliability reasons.

Table 4.7.: Required DAL and redundancies for TARMS.

ARC	DAL	Redundancy
b	none	No
c	D	No
d	C	Yes

4.3. Architectures

The visualized architectures evolve from the required components listed in section 4.1 and the redundancies listed in section 4.2. The ARC or Termination variants are not considered here. To visualize the architectures, the legend shown in figure 4.4 is applied.
Components are illustrated with boxes. Multiple components such as actuators for the different control surfaces are illustrated as a second box beyond the main box. Redundant components are illustrated with a second box behind the main box.

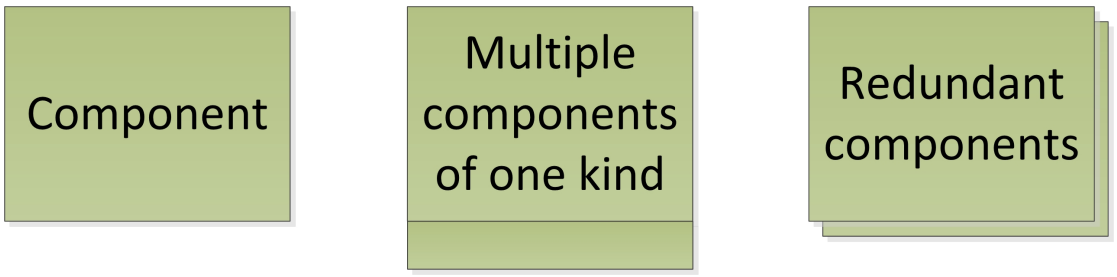


Figure 4.4.: Key for interpreting the architectures shown in Fig. 4.5 to 4.8.

The simplest architecture is for SAIL III. Only ARC-b is possible here. The architecture is shown in figure 4.5.

For SAIL IV a MDS is added. In addition, missions with ARC-c are possible in this variant. The architecture is shown in figure 4.6.

The SAIL V or VI architecture differs mainly in the necessary redundancies. In addition, no monitoring system is implemented. With this architecture all ARCs can be flown if the sufficient TARMS is implemented. The architecture is shown in figure 4.7.

The architecture for a certified system is similar to the SAIL V or VI architecture. The FCS is replaced with a FCELS and the IDRS has been removed. The architecture is shown in figure 4.8.

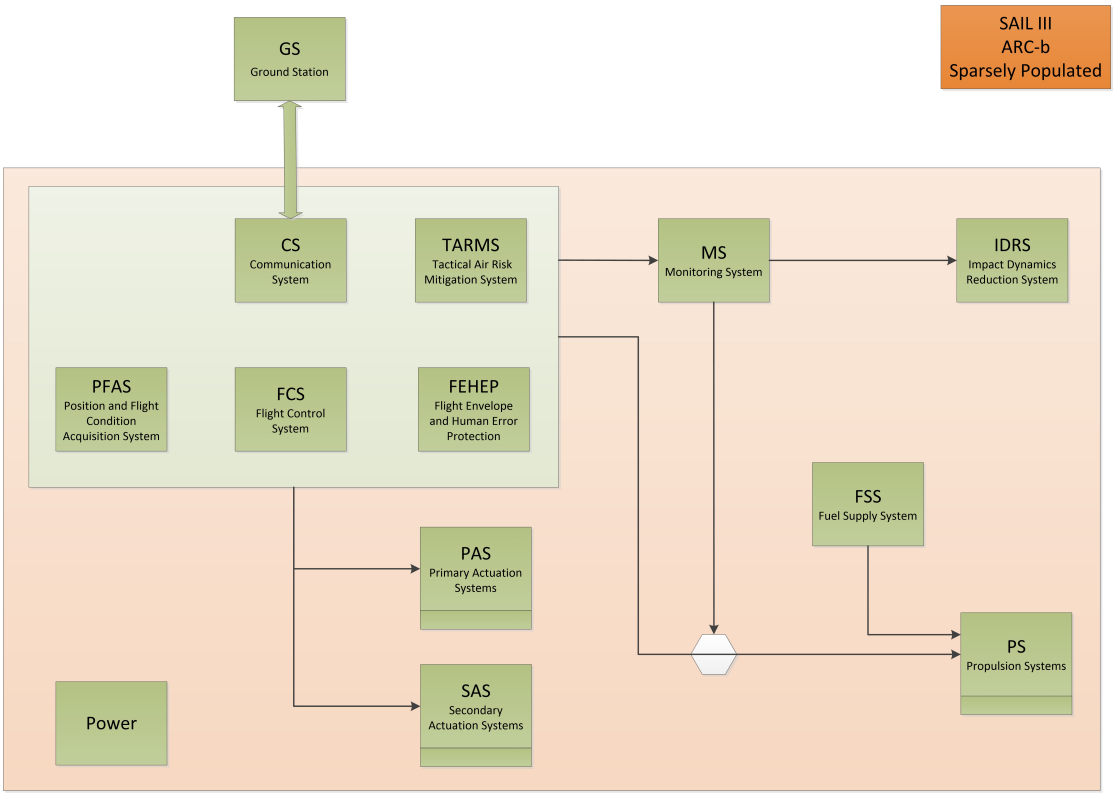


Figure 4.5.: Architecture for SAIL III.

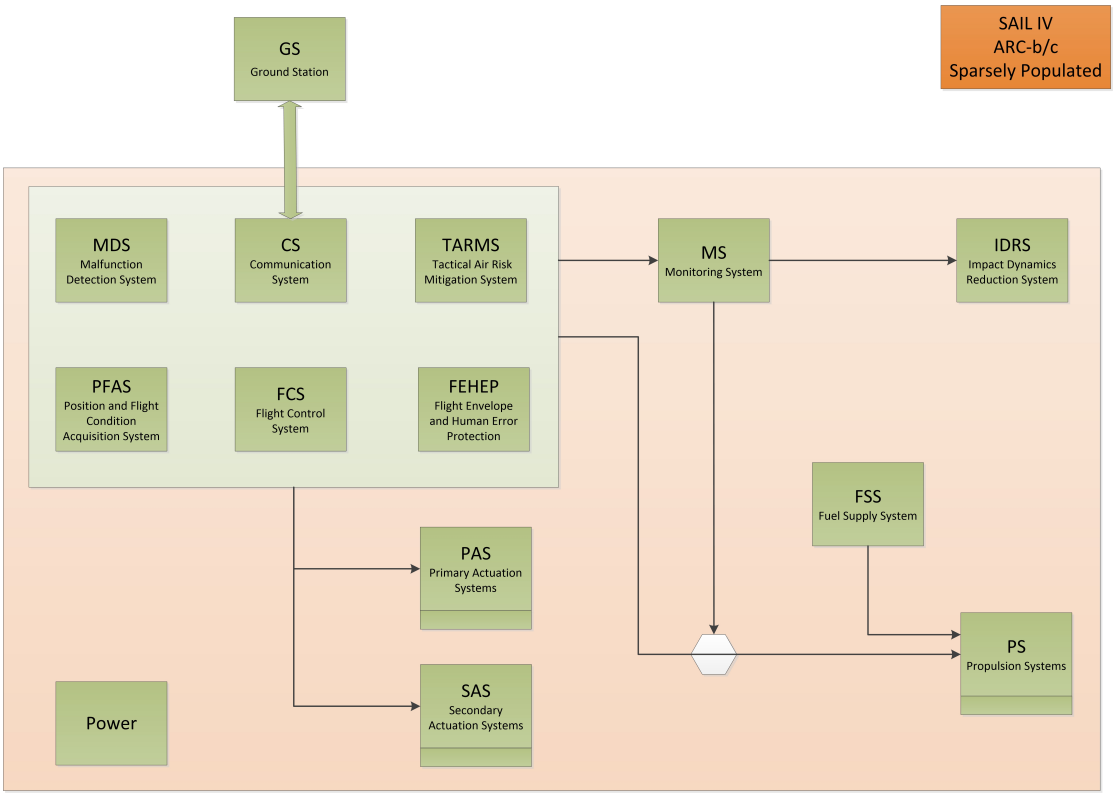


Figure 4.6.: Architecture for SAIL IV.

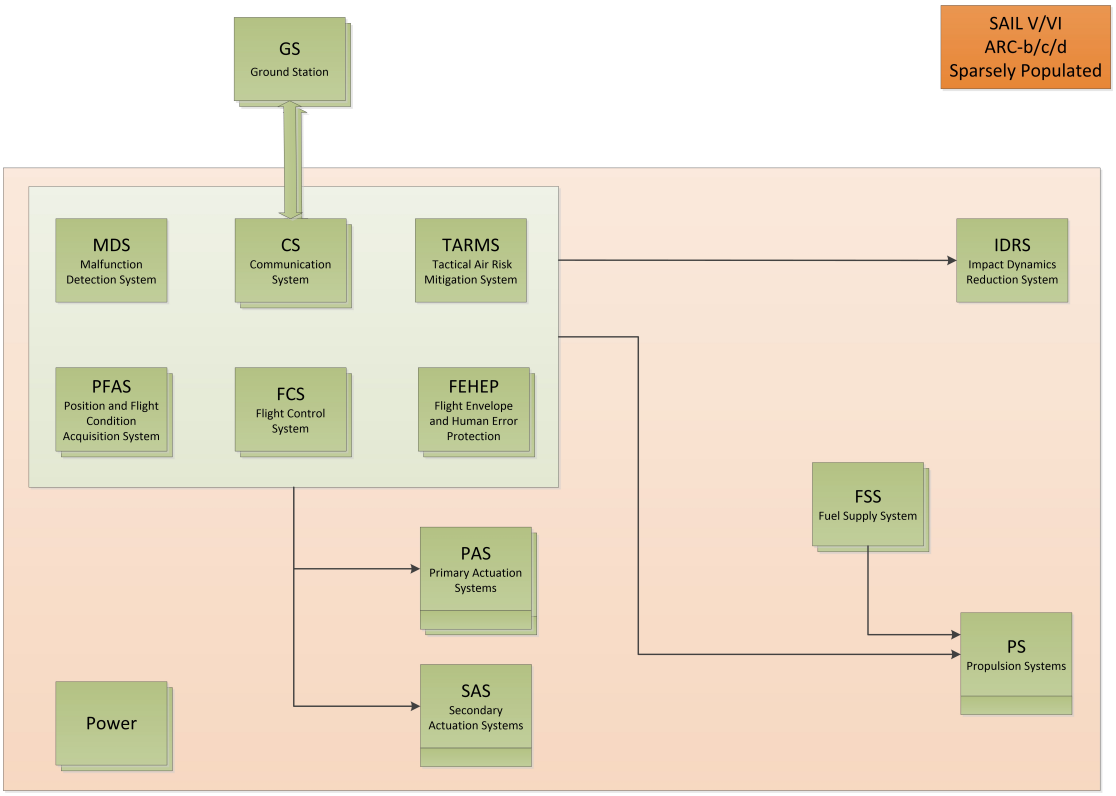


Figure 4.7.: Architecture for SAIL V.

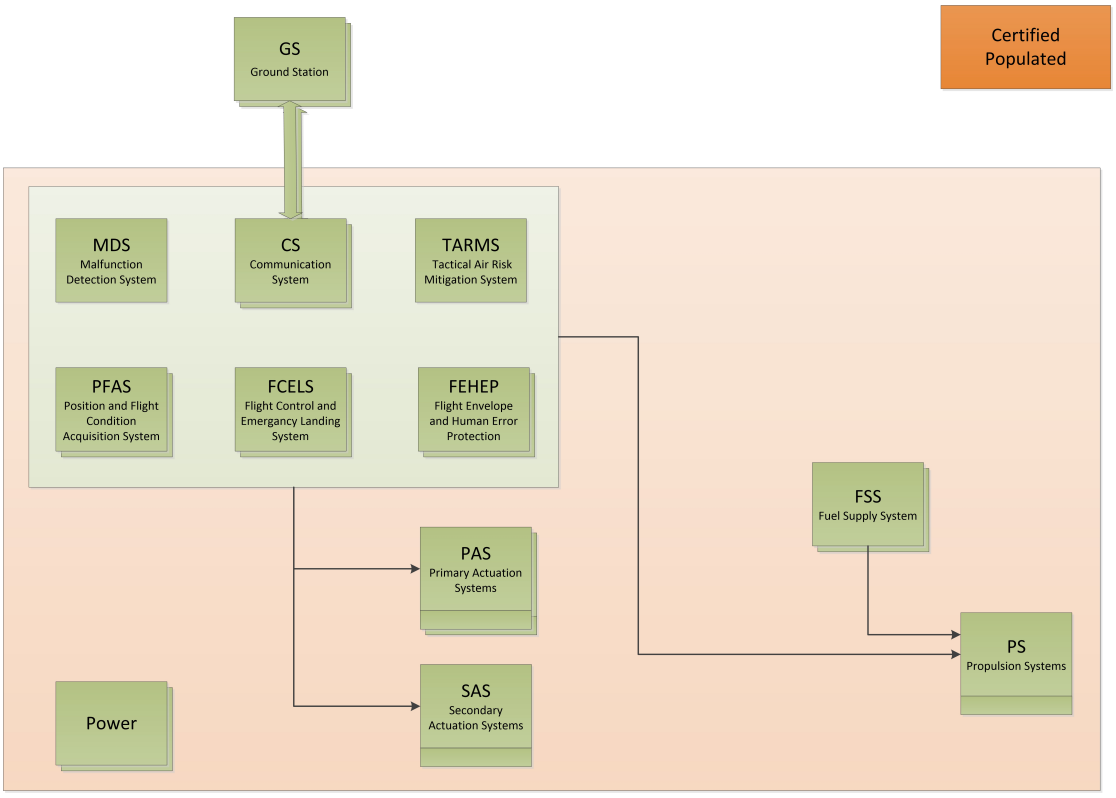


Figure 4.8.: Architecture for a certified System.

4.4. Effort Estimation

From the number of system architectures found, one architecture is selected for further consideration. The choice has to be made considering the overall mission effects. One input are the vehicle acquisition cost, which are highly depending on the chosen system architecture. Without further developed design, specific numbers on cost cannot be given. But architecture and requirements give the possibility to estimate a simple relative effort among the variants. In the following the development effort for the different architectures is compared. Because the architectures are taken as basis for this estimation, the resulting numbers describe only the development effort of the system architecture and no structural components or elements like gears or engines.
A relative effort estimation E_{rel} for each developed system architecture can be found by scoring each of the n components and summarizing the points to find a nondimensional development effort. The sum is then divided by the points of a reference architecture to find a relative value.
The points for each component are found due to its functional complexity, its required DAL and redundancy, if applied. The functional complexity gives a basic number which is then multiplied with factors for the DAL and redundancy. Consequently E_{rel} is calculated by

$$E_{rel} = \sum_{i=1}^{n} \frac{B_i \cdot f_{a,i} \cdot f_{DAL,i} \cdot f_{r,i}}{P_{ref}}. \tag{4.1}$$

The base for the analysis is the basic functional complexity of each component B_i. The estimation used evolves from the number of general tasks of each component to be conducted and can be found in table 4.8. Components which contain a high amount of commercial off the shelf products were considered less sophisticated. The listing of the general tasks of each component can be found in Appendix A.

Table 4.8.: Points for the basic functional complexity of each component.

Components	B_i	**Components**	B_i
CS	2	TARMS-c	4
FCS	5	TARMS-d	8
FCELS	7	PAS	4
FEHEP	4	SAS	2
GS	4	FSS	3
Link	3	PS	2
MDS	4	MS	6
PFAS	4	IDRS	3
TARMS-b	2	Power	3

The factor $f_{a,i}$ describes if a component is used in the architecture. It is 1 if it is and 0 if it is not. The usage of a component in a certain architecture can be found in section 4.1.
The factor for the complexity depending on the DAL $f_{DAL,i}$ was found by reviewing a report from RockwellCollins [8]. The different approaches were averaged to a factor of 1.5 for each following DAL. This simplified factor disregards important but unknown influences like team experience. It is assumed that this factor can be applied for all subjects. The factor for each DAL can be found in table 4.9.

Table 4.9.: Effort factors for different DAL.

DAL	f_DAL, i
None	1
D	1.5
C	2.25
B	3.38

The factor for the complexity depending on the redundancy $f_{r,i}$ is assumed to be at least the double effort of a simplex system. It is assumed that the additional testing required for verifying interdependencies increases this factor to 3.
The resulting numbers are divided by a reference value P_{ref} to find a relative value. The number of SAIL IV, ARC-c, TV 1 is chosen as reference value because it is the preliminary preferred variant within SORA as described below. The final relative values can be found in figure 4.9.

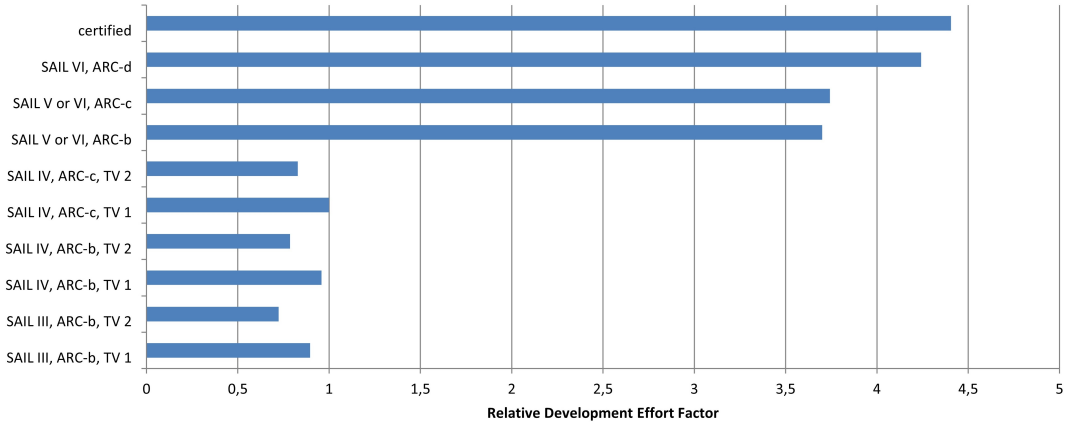


Figure 4.9.: Relative Development Effort Factor for different architectures.

Figure 4.9 shows that the architectures can be categorized into two groups: Architectures evolving from SAIL III or IV and architectures evolving from SAIL V or IV or a certified system. The leap between the two groups is mainly driven by OSO #5. This OSO requires failure conditions to occur with a certain probability which leads to an increased DAL and required redundancy.
The development effort is more dependent on the SAIL than the ARC. An exception is ARC-d which increases the development effort significantly. If a termination is possible, the termination variant has significant impact on the development effort. The challenging requirements of SAIL V and VI differ by just a small increase of the development effort to a certified system, if ARC-d is to be used. For further analysis it seems useful to reduce the number of considered architectures. If a complex and highly reliable system shall be developed, it seems beneficial to choose a certified system. The development effort is just slightly higher than a SAIL V or VI system, but has no restrictions for operation over populated areas, which will shorten many routes or enable scenarios entirely. If a simple system shall be developed, it seems valuable to aim for SAIL IV and ARC-c. Further requirement reduction by using more mitigations will not reduce the development effort significantly, but restrict the flown missions. It is assumed that the use of termination variant 2 could restrict the route and this restriction does not justify the lower development effort. Therefore, SAIL IV, ARC-c, TV 1 is chosen.

The given results can be used as a support for architectural decisions. However, it is important to note that many simplifications were made to find these numbers and that these numbers can significantly differ in a specific project. A big influence is the team experience in developing systems with design standards and DAL. Some systems may also react sensible to additional mass from

redundant systems which was not covered in this analysis and could have an impact on the feasibility. Finally, the input parameters cannot be attested as free from subjectivity. Nevertheless, the given tendencies and especially the statement that a SORA system should stay within SAIL IV can be used for further development.

5 Conclusion

This work developed system architectures and estimated related development efforts for ALAADy configurations based on safety requirements derived from SORA. Possible architectures were diversified depending on the SAIL, the Air Risk Class (ARC) and, if applied, the Termination Variant (TV). Two TVs were found to satisfy the SORA requirements which generate slightly different requirements for the architectural components. The different architectures were analyzed regarding their crucial components, including the components Design Assurance Level (DAL) as well as necessary redundancies. The related development effort was estimated by scoring the individual components. There was a big discrepancy found between SAIL IV and V, which indicates that the costs of applying additional mitigations will be much smaller than the increased cost of a system for a higher SAIL. This evolves from the requirement to fulfill certain probabilities of failure conditions which will be similar to the ones of a certified system. This explains the small difference between SAIL VI and a certified system, too. It is likely that processes for certified systems will be adapted to fulfill this requirement within SORA. Consequently, this could lead to a situation where certified systems will be preferred to systems of SAIL V and VI.
SAIL IV with a high ARC or a certified system is found to be best suitable for ALAADy missions. Which of these different approaches is finally the best has to be examined in further considerations which have to be highly integrated within economical, technical and operational perspectives. This could change some statements within this work because they evolve from safety requirements and not economically driven reliability.
The developed architectures and effort estimations give the possibility to take them as an input for further economic models for the targeted operation. This information can be used to iterate payload mass, velocity and mission scenarios. In a feedback loop information about necessary reliability for an economic operation could be considered. The results indicate that ALAADy configurations seem to be operated best in either SORA Specific Assurance and Integrity Levels (SAIL) IV with the highest possible ARC or as a certified system. This postulate has to be further examined. If confirmed, the focused systems should be further considered with holistic development plans to detail the results. Furthermore, the results in this work are based on SORA 2.0. Eventually, there will be more Annexes published or further versions which will have to be incorporated into the existing work. The comparison to a certified system can be evaluated in more detail when a certification specification for certified UAS is available.
The results are based on assumptions which have to be considered further. There is a possibility that some of the significant statements evolve from the used methodology and do not mirror the reality. Therefore, a detailed development of the architectures needs to be realized in the future. Further work should also consider the influence of team experience in developing systems following standards and the possible reduction of DAL B systems to DAL C systems, when using independent redundancies.

Bibliography

[1] JARUS. JARUS guidelines on Specific Operations Risk Assessment (SORA). Edition 2.0, 2019.

[2] Project internal work within ALAADy.

[3] EU. Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, 2019.

[4] F. Nikodem, J. S. Dittrich, A. Bierig. The new Specific Operations Risk Assessment approach for UAS regulation compared to common civil aviation risk assessment, 2018.

[5] SAE Aerospace. ARP4754A: Guidelines for Development of Civil Aircraft and Systems, 2010.

[6] JARUS. AMC RPAS.1309: Safety Assessment of Remotely Piloted Aircraft Systems. Issue 2, 2015.

[7] SAE International. ARP4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996.

[8] RockwellCollins. Certification Cost Estimates for Future Communication Radio Platforms, 2009. https://docplayer.net/13974967-Certification-cost-estimates-for-future-communication-radio-platforms.html. Accessed 02 December 2019.

List of Figures

List of Tables

List of Symbols

Formula Symbols

B_i	Non-dimensional basic functional complexity of each component	–
E_{rel}	Non-dimensional relative effort estimation	–
$f_{a,i}$	Factor of 0 or 1 if a component is used in the considered architecture	–
$f_{DAL,i}$	Effort factor for different DALs	–
$f_{r,i}$	Effort factor for redundancy	–
n	Number of components	–
P_{ref}	Non-dimensional points of a reference architecture	–

Abbreviations

ALAADy	Automated Low Altitude Air Delivery
AMC	Acceptable Means of Comliance
ARC	Air Risk Class
BVLOS	Beyond Visual Line of Sight
CS	Communication System (closer described in 3.3.1)
DAL	Design Assurance Level
DLR	German Aerospace Center, Deutsches Zentrum für Luft- und Raumfahrt
ERP	Emergency Response Plan
EU	European Union
FCELS	Flight Control and Emergency Landing System (closer described in 3.3.1)
FCS	Flight Control System (closer described in 3.3.1)
FEHEP	Flight Envelope and Human Error Protection (closer described in 3.3.1)
FH	Flight Hour
FSS	Fuel Supply System (closer described in 3.3.3)

GNSS	Global Navigation Satellite System
GRC	Ground Risk Class
GS	Ground Station (closer described in 3.3.1)
HMI	Human Machine Interface
IDRS	Impact Dynamics Reduction System (closer described in 3.3.4)
IMU	Inertial Measurement Unit
MASPS	Minimum Aviation System Performance Standard
MDS	Malfunction Detection System (closer described in 3.3.1)
MOPS	Minimum Operational Performance Standards
MS	Monitoring System (closer described in 3.3.4)
OSO	Operational Safety Objectives
PAS	Primary Actuation Systems (closer described in 3.3.2)
PFAS	Position and Flight condition Acquisition System (closer described in 3.3.1)
PS	Propulsion Systems (closer described in 3.3.3)
SAIL	Specific Assurance and Integrity Levels
SAS	Secondary Actuation Systems (closer described in 3.3.2)
SORA	Specific Operation Risk Assessment [1]

TARM	Tactical Air Risk Mitigation
TARMS	Tactical Air Risk Mitigation (TARM) System (closer described in 3.3.1)
TV	Termination Variant
UAS	Unmanned Aircraft System
VLOS	Visual Line of Sight

A General Tasks for each component

Communication System (CS):

- Gather Data
- Share Data

Flight Control and Emergency Landing System (FCELS):

- Autopilot
- Actuator control
- Flight path generation from waypoints
- Direct steering
- Emergency Landing

Flight Control System (FCS):

- Autopilot
- Actuator control
- Flight path generation from waypoints
- Direct steering

Flight Envelope and Human Error Protection (FEHEP):

- Restrict flight attitude
- Restrict flight path to comply with allowed flight geography
- Restrict flight velocity
- Provide correction maneuvers

Fuel Supply System (FSS):

- Provide fuel to Propulsion Systems (PS)
- Switch between tanks
- Provide possibility for fuelling

Ground Station (GS):

- Show flight Information on HMI
- Provide waypoints to vehicle
- Provide direct steering to vehicle
- Recognize faulty vehicle parameters

Impact Dynamics Reduction System (IDRS):

- Ensure passively stable flight mode

Link:

- Send data
- Reeceive data
- Check connection

Malfunction Detection System (MDS):

- Read temperature and pressure data
- Recognize faulty vehicle parameters
- Recognize faulty systems

Monitoring System (MS):

- Provide power from one or multiple battery systems
- Send monitoring data
- Provide charging capabilites
- Calculate position from one or multiple Global Navigation Satellite System (GNSS)
- Calculate position and flight attitude from one or multiple Inertial Measurement Unit (IMU)
- Calculate flight altitude and velocity from pressure sensors

- Combine information from single systems
- Check adherence to allowed status
- Trigger flight termination

Primary Actuation Systems (PAS):

- Receive steering data
- Control actuator
- Send monitoring data

Position and Flight condition Acquisition System (PFAS):

- Calculate position from one or multiple GNSS
- Calculate position and flight attitude from one or multiple IMU
- Calculate flight altitude and velocity from pressure sensors
- Combine information from single systems

Power:

- Provide power from one or multiple battery systems
- Send monitoring data
- Provide charging capabilites

Propulsion Systems (PS):

- Receive power setting data
- Control motors
- Send monitoring data

Secondary Actuation Systems (SAS):

- Receive steering data
- Control actuator
- Send monitoring data

Tactical Air Risk Mitigation (TARM) System (TARMS)-b:

- Recognize other aircraft
- Send simple avoid commands

Tactical Air Risk Mitigation (TARM) System (TARMS)-c:

- Recognize other aircraft
- Send avoid commands

Tactical Air Risk Mitigation (TARM) System (TARMS)-d:

- Recognize other aircraft
- Send complex avoid commands
- Communicate position and flight attitude data to other aircraft